UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/390,362	09/07/1999	SCOTT ALEXANDER VANSTONE	06944.0017	6724

293 7590 04/26/2006

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave
Suite 406
Alexandria, VA 22314

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/390,362	VANSTONE ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/5/2006 has been entered.

Claims 1-13 are pending.

Response to Amendment and Arguments

Applicant's amendments and arguments have been considered, but are moot in view of new grounds of rejections presented below.

Claim Objections

Claim 1 is objected to because of the following informalities: In line 7 of claim 1, the examiner believes "bitstring" should be "bit string". Appropriate correction is required.

Specification

The disclosure is objected to because of the following informalities: On page 3, in the paragraph beginning on line 12, it is disclosed that "Each of the cryptographic units 16, 18 implements a public key encryption scheme that enables it to generate a session key, to encipher or decipher a message using the session key or sign a message using a private key which can then be recovered using a corresponding public key." The way this sentence is written, it would appear that applicant is saying that a private key can

be recovered using a corresponding public key. However, the examiner believes that applicant may have meant that it is the message that is recovered using a corresponding public key. It is well known and understood by one of ordinary skill that in asymmetric cryptosystems, one should not be able to obtain a private key from the public key. If one were able to do so, this defeats the entire idea behind asymmetric cryptography of being able to make the public key public without fear of the private key being compromised.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 1 recites in lines 3-4, "...and available to the other of said pair of correspondents...". It is unclear what is available to the other of said pair of correspondents. The examiner will assume applicant is referring to the public key since in a public/private cryptosystem, the private key is kept secret while the public key is shared.

2. As per claim 1, the limitation recited in lines 7-8 is indefinite. Note that first signature component c is computed using first plaintext bit string H. First plaintext bit string H is disclosed both earlier in the claim and in applicant's specification as being a subsection of the plaintext message. It is unclear how the entire plaintext message can be hidden in c as line 8 seems to be implying if c was derived from H and H was only derived from a portion of the plaintext and not the entire plaintext. Applicant may have meant that a portion of the plaintext is hidden in c, i.e. the portion consisting of H. A similar problem exists with regards to the limitation recited in lines 11-12. That which was used to derive second signature component s was merely a portion of the overall plaintext message, so it is indefinite how the plaintext, i.e. the entire plaintext message, could be hidden in s. The closest interpretation the examiner can come up with where the limitations as currently recited makes some sense is that since the components H and V are part of the original plaintext and not the entire plaintext, the plaintext has been hidden by the division of the plaintext and as such, any component derived from H and V would also have the plaintext hidden in the component. Note that applicant's specification discloses that only H is the hidden part while V is the visible part, so this interpretation seems unlikely as what applicant may have meant.
3. As per claim 1, the examiner notes that the last limitation recited therein does not necessarily limit the claim. The examiner can apply at least two separate interpretations to the limitation. In the first interpretation, said second plaintext bit

string V being referred to in the last limitation is available during verification in that it is a discrete component of the signature (s, c, V). This interpretation further limits the claim because it empathizes that the signature is composed of three discrete components, s, c, and V, each separately accessible. In the second interpretation, the limitation merely states that V is available as an input to the verification protocol, though not necessarily by parsing it from the signature first. In light of the specification disclosing the signature being comprised of the components being concatenated together, the examiner suspects applicant meant for the first interpretation to apply. However, the examiner cannot read limitations from the specification into the claim. Since both interpretations seem to be equally valid, clarification is respectfully requested.

4. Claim 7 recites "said components" in line 7, which lacks antecedent basis.
5. Claim 7 recites "said one component" in line 9, which lacks antecedent basis. The dependent claims of claim 7 also recite "said one component" which also lacks antecedent basis. It is unclear if applicant was referring to one of the components in the set of discrete components recited in line 4 and if so, which one(s).
6. Claim 7 recites "said combination" in line 11, which lacks antecedent basis. It is unclear if the combination that "said combination" is referring to is the resultant of the combining in lines 9-10.
7. Claim 12 recites that "said function is encryption with a key, said key is recoverable from said signature, said complementary function is decryption with

said key." Claim 13 recites that "said key is a short-term public key derived from a short-term private key used in the provision of said second signature component." Claim 12 as recited appears to imply that encryption and decryption was done using the same key. However, claim 13 implies that said key as recited in claim 12 was a public key derived from a private key. One of ordinary skill should appreciate that in a public/private key system, encryption is done using one key and decryption is done using the other key of the key pair. One cannot both decrypt and encrypt using just the public key. It is unclear how encryption and decryption is done using the same public key recited in claim 13.

8. As per claim 12, it is unclear how a key is recoverable from said signature. It does not appear that applicant's specification discloses how this can be done. The examiner believes applicant may have meant that the message or part of the message, i.e. such as the first plaintext bit string H, is recoverable from said signature instead of the key. Note that pages 3-4 of applicant's specification discloses recovering a bit string H' from the signature of applicant's invention, not a key.
9. Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 7-8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As per claim 7, it is unclear that the steps of the method of claim 1 yield a concrete, useful, and tangible result. As such, it is not statutory. Note that the method is directed towards the practical application of verifying a plaintext message. Applicant's specification implies that verification that a signature is valid occurs when the required redundancy is detected in a signature (p3, lines 3-5 and p6, lines 3-6). A search of the prior art also shows that others in the field of computing and cryptography used the detection of redundancy in a signature as a verification of a signature (see Rueppel et al US 5,600,725). However, note that in the last limitation of claim 7, H is examined for a predetermined characteristic. A predetermined characteristic is not necessarily redundancy, thus verification does not necessarily occur upon the detection of the predetermined characteristics. Because the method does not necessarily accomplish verification, the method does not have a concrete, useful, and tangible result. Claim 8 is also non-statutory for the same reasons. Claim 9 is statutory because applicant has defined that the predetermined characteristics is redundancy. It inherently flows, based on what is disclosed in applicant's specification (and what is disclosed by Rueppel as being known to one of ordinary skill), that claim 9 yields a concrete, useful, and tangible result because in examining H for the predetermined characteristics of redundancy, the signature would be verified if redundancy is found.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 and 7-8 are rejected under 35 U.S.C. 102(b) as being anticipated by ISO/IEC 9796-2, herein referred to as ISO2.

Claim 1:

ISO2 discloses:

1. Subdividing said plaintext message into a first plaintext bit string H and a second plaintext bit string V (p5, section 6.3.2.2).
2. Utilizing said first plaintext bit string H to compute a first signature component c, in which the plaintext is hidden (p5, sections 6.3.2.2-6.3.3).
3. Forming from said first signature component c and said second plaintext bit string V, an intermediate signature component c' (p5, section 6.3.3-6.3.4).
4. Utilizing said intermediate signature component c' and said private key a to provide a second signature component s, in which the plain text is hidden (p5, section 6.3.3-6.3.4).
5. Forming a signature (s, c, V) by including said first signature component c, said second signature components s, and said second plaintext bit string V as discrete signature components (p5, section 6.4)

6. Whereby during verification, said second plaintext bit string V is available as an input to a verification protocol (p6, section 7.3.4).

Note that in partial recovery the signature is Σ with Mn. Mn is equivalent to V as recited in the claim. Σ was derived from Sr, which was derived from Si, which was derived from Mr. Mr is equivalent to H as recited in the claim. One can view Si as c and Sr as c'. Note that the limitation of forming a signature by including the components as discrete signature components is very broad. One should appreciate that though some of the above components are derived from other components, they are also individually discrete components. However, because they are derived from other components, in including a component in the signature, one is also including the subcomponent the component was derived from in the signature. The examiner respectfully suggests applicant more clearly define what is meant by the term "including" as used in the claim or use a different term to describe applicant's invention.

Claim 7:

ISO2 discloses:

1. Combining one component with said second plaintext bit string V (p5, section 6.3.3-6.4 and Table 1).
2. Recovering said first plaintext bit string H from said combination using publicly available information of the purported signer including said public key (p6, secion 7.2).

3. Examining said recovered first plaintext bit string H for a predetermined characteristic (p6, section 7.3.4).

The examiner notes that applicant incorporated features similar to what is recited in claim 1 to the preamble of claim 7. However, it would appear that the steps of the method do not depend on the preamble for completeness. The steps by themselves could be carried out using other types of messages and components not defined by what was intended in the preamble, thus the steps could stand alone. As such the preamble is not given patentable weight since it appears the preamble merely defines the type of message and components intended to be used by the steps of the method, see In re Hirao, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and Kropa v. Robie, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Claim 8:

ISO2 further discloses wherein said combination of said one component and said second plaintext bit string V includes hashing a combination of said one component and said second plaintext bit string V (p5, section 6.3.3-6.4 and Table 1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP 0918274) in view of applicant's admittance of prior art.

Claim 1:

McCollom discloses:

7. Subdividing said plaintext message into a first plaintext bit string H and a second plaintext bit string V (col 4, lines 42-43).
8. Utilizing said first plaintext bit string H to compute a first signature component c, in which the plaintext is hidden (col 4, lines 45-47).
9. Forming from said first signature component c and said second plaintext bit string V, an intermediate signature component c' (col 4, lines 47-50).
10. Utilizing said intermediate signature component c' and said private key a to provide a second signature component s, in which the plain text is hidden (col 4, lines 50-52).
11. Forming a signature utilizing the signature components (col 4, lines 52-56).

McCollum does not disclose the signature was formed by including said first signature component c, said second signature component s, and said second plaintext bit string V as discrete signature components, whereby during verification, said second plaintext bit string V is available as an input to a verification protocol.

However, applicant discloses in applicant's specification that at the time applicant's invention was made, it was well known in the art to form a signature by

including three discrete signature components, whereby during the verification, said plain text bit string V, i.e. the visible component, is available as an input to a verification protocol, i.e. recovery process (p1, last paragraph-p2, line 9). On page 2, one can see that the well known signature included discrete signature components H, SHA1(V), and I_A.

One of ordinary skill should appreciate that since claim 1 recites that first plaintext bit string H is utilized to compute c, this limitation is broad enough such that it reads on c and H being the same. One can see on page 2 that the well known signature disclosed therein has a discrete component derived from V. The examiner notes that in reading applicant's specification, this is probably not what applicant meant by using the term "including" in the claim, but the examiner submits that "including" is an extremely broad term and is broad enough to encompass including V by including the hash value of V as a component of the signature. As per the second signature component s, the examiner submits that the identifier of the signer I_A can read on this. Claim 1 recites that s was formed by utilizing c' and a private key to derive s; c' was formed using c and V. One of ordinary skill should appreciate that s as disclosed by McCollum can function as an identifier for the signer since only the signer should have the private key, thus anything which was encrypted using the private key of the signer identifies that the signer was the one who performed the encryption.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to combine McCollom's teachings with what applicant discloses as being well known in the art according to the limitations recited in claim 1. One of

ordinary skill would have been motivated to modify McCollom's teachings according to the limitations recited in claim 1 because if done properly, it could increase bandwidth efficiency and reduce data storage.

Claim 6:

McCollom further discloses said signature component s is generated by hashing said first signature component c and said second plaintext bit string V (col 4, lines 45-52).

Claim 11:

McCollom does not explicitly disclose wherein said first signature component c is formed by applying a function to said first plaintext bit string H and said first plaintext bit string H may be recovered from said first signature component c by applying a complementary function to said first signature component c. However, one of ordinary skill should appreciate that the limitation recited in claim 1 which describes how c was formed from H is very broad, i.e. "utilizing said first plaintext bit string H to compute a first signature component c". One of ordinary skill should appreciate that using the value of H as the value of c reads on the limitation. In doing this, one is applying an identity function to the value of H. For example, in multiplication 1 is an identity function because anything multiplied by 1 is the number itself. The complementary function of an identity function is the identity function itself. The examiner submits that using the value of H as the value of c reads on the limitation recited in claim 1. One of ordinary skill would have been motivated to use the value of H as the value of c because it would

mean one less calculation that has to be performed in signature calculation, speeding up the process of signature calculation.

Claim 12:

As per claim 12, McCollom does not disclose wherein said function is encryption with a key, said key is recoverable from said signature, and said complementary function is decryption with said key. However, it would appear that applicant discloses that this limitation was well known in the art at the time applicant's invention was made (specification: p3, lines 12-18).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify McCollom's invention according to the limitations recited in claim 12. One of ordinary skill would have been motivated to do so because the use of encryption in the signature using a key known only to the sender would ensure that no one could impersonate the sender without being exposed as a fraud.

Claim 13:

McCollom does not disclose wherein said key is a short-term public key derived from a short-term private key used in the provision of said second signature component. However, the examiner asserts that public/private key cryptosystems, i.e. asymmetric cryptosystems, were well known in the art at the time applicant's invention was made. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify McCollom's invention according to the

limitations recited in claim 13 because public/private key cryptosystems tend to be more secure than symmetric key cryptosystems since they usually use longer keys.

Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP 0918274) in view of applicant's admittance of prior art and further in view of ISO/IEC 9697-1, herein referred to as ISO1.

Claim 2:

McCollom does not disclose wherein redundancy in said first plaintext bit string H is compared to a predetermined level prior to computing said first signature component c. However, ISO1 implicitly discloses this limitation (p1, third paragraph). At the time applicant's invention was made, it would have been obvious to further modify McCollom's invention according to the limitations recited in claim 2. One of ordinary skill would have been motivated to do so because it is common in the prior art (as evidenced by Rueppel: abstract) to validate a signature based on the redundancy contained in a message. By checking at least part of a message for redundancy of a predetermined level prior to computing a signature component, one would ensure that the message contained enough redundancy that once the signature is formed, the redundancy can be detected. Otherwise, if there is not enough redundancy, one would be wasting time forming a signature that does not have enough redundancy that could be used to validate the formed signature.

Claim 3:

ISO1 further discloses wherein said redundancy is adjusted to exceed a predetermined level (p1, third paragraph). One of ordinary skill would have been motivated to incorporate this teaching within McCollom's modified invention because it would ensure the signature would have enough redundancy to be used for validation.

Claim 4:

ISO1 further implicitly discloses wherein data is added to said first plaintext bit string H to adjust said redundancy (p1, third paragraph).

Claim 5:

ISO1 further implicitly discloses wherein an indicator is included in said first plaintext bit string H to indicate additional data (p1, third paragraph). Note that ISO1 discloses that during the verification process, the artificial redundancy is revealed, implying that there was an indicator which allowed one to know what is the redundancy and what is not.

Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over ISO/IEC 9796-2, herein referred to as ISO2, in view of Rueppel et al (US 5,600,725).

Claim 9:

ISO2 does not explicitly disclose wherein said predetermined characteristic is the redundancy of said recovered first plaintext bit string H. However, Rueppel discloses validating a signature by detecting redundancy in a text string (abstract and col 2, lines

40-41). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify ISO2's invention according to the limitation recited in claim 9 in light of Rueppel's teachings. One of ordinary skill would have been motivated to do so because detecting redundancy to verify a signature was a standard way of verifying a signature at the time applicant's invention was made.

Claim 10:

ISO2 further discloses wherein said signature includes a third component derived from a combination of said one component and said second plaintext bit string V (p5) and said first plaintext bit string H is recovered utilizing said third component (p8, section A.5).

Note that Σ derived from several components and in that manner there is a third component that is included in the signature, which was derived from a combination of said one component and said second plaintext bit string V. In verifying the signature, Σ is input into a verification function (p8, section A.5). In a partial recovery scheme, one should appreciate that the message or part of the message is in the signature (Introduction). Since Σ is input into a verification function to verify the signature, one should appreciate that H would be recovered from the signature utilizing Σ, thus utilizing said third component.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

PP

HOSUK SONG
PRIMARY EXAMINER